AIR WAR COLLEGE

AIR UNIVERSITY

COMMAND AND CONTROL ACROSS SPACE AND CYBERSPACE DOMAINS

by

Jason A. Parish, CDR, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Michael Ivanovsky

16 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Commander Jason A. Parish is assigned to the Air War College, Air University, Maxwell AFB, AL.

His sea duty assignments include tours as anti-submarine warfare officer in USS Taylor (FFG 50), navigator in USS Vicksburg (CG 69), combat systems officer in USS Independence (LCS 2), and assistant chief of staff for command, control, communications, computers, and intelligence (C4I) on the Expeditionary Strike Group SEVEN (ESG 7) staff.

Ashore, Parish served as associate dean/executive officer of faculty and staff development, Defense Language Institute Foreign Language Center, resource operations coordinator then deputy chief of vehicle operations and engineering within the operations branch of the NRO, distance support department head, LCSRON ONE, and executive officer, NIOC Sugar Grove.

Parish attended Rensselaer Polytechnic Institute graduating with a Bachelor of Science in Environmental Engineering, and the Naval Postgraduate School earning a Master of Science degree in Space Systems Operations.

His personal awards include the Defense Meritorious Service Medal, Meritorious Service Medal, Joint Service Commendation Medal, Navy and Marine Corps Commendation Medal, and the Navy and Marine Corps Achievement Medal along with various unit and service awards.

Abstract

How can command and control across the space and cyberspace domains be improved? The question is important because the unique challenges to command and control when functional missions cross space and cyberspace domains can lead to confusion and mistakes when command and control responsibility is unclear.

In this paper I compared and contrasted doctrinal methods to command and control in the space and cyberspace domains. I evaluated published methods to determine their effectiveness and provided recommendations based on my findings.

I also gathered and considered opinions expressed in multiple articles published in journals, magazines, periodicals and professional online websites. I evaluated the opinions on validity and efficiency by contrasting the suggested command and control methods with methods proposed by others and current practices.

When my research was complete, I had sufficient background to form a method to improve command and control across the space and cyberspace domains. I applied what I learned to answer three questions: (1) where does space operations stop and cyberspace operations begin; (2) who has the lead (command) where space and cyberspace operations meet; and (3) which mission area has priority when space and cyberspace operations conflict. Then I made recommendations for improving or changing current methods of command and control across those boundaries.

Introduction

"Every weapon system we build is critically dependent on cyber, critically dependent on space--and I use those terms interchangeably because they're critically dependent on network information getting into their system."[1]

-- Gen John E. Hyten, Commander, Air Force Space Command

Warfighters are reliant on space and cyberspace for operational coordination and tactical impact. Due to their unique characteristics (global reach, unrestricted by sovereign boundaries), there are challenges associated with command and control across the space and cyberspace domains. Space and cyberspace operations conducted at the strategic level can cause ripples felt at the operational and tactical levels. Unawareness of the impact of actions taken at the strategic level can cause confusion and misunderstandings at the operational and tactical levels when space and cyberspace users find themselves without assets and services they rely on. Confusion and misunderstandings can lead to mistakes with dire consequences.

In a recent article published by Breaking Defense, Maj Gen Zabel, in response to the question, "If the tech guys urgently need to shut a system down — say, because it's infected with a virus and they want to stop it spreading — but the combat commanders need it to run their operations, who prevails?" responded with, "Frankly, it is a question I have myself."[2]

Maj Gen Zabel said the hypothetical scenario was not complex enough and continued, "For example, to detect, track, and target an incoming ICBM, ballistic missile defense depends on a constant feed of intelligence from satellites, ships, and ground-based radars. None of these sensors belong to the Ground-Based Interceptor units that are supposed to shoot the ICBMs down. If DISA's cyberwarriors decide they need to, say, update a vital piece of software, how do they make sure the potential disruption is acceptable, not only to the people who own the

satellites, ships, and ground radars, but to the third parties who depend on them, like missile defense units?"[3]

Thesis

Clear and concise command and control guidance in the space and cyberspace domains will mitigate confusion and minimize mistakes within and across these domains.

Warfare Domains

The United States military operates in five warfare domains: land, maritime, air, space and cyberspace. Four of these domains (land, maritime, air and space) are physical domains, but cyberspace has non-physical traits with global reach within the information environment.[4]

Land Domain

The land domain is defined in Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations* as, "The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals."[5] The land domain is constrained by the sea and the geographic sovereignty of nation states. Land forces generally consist of Army, Marine or special operations units conducting operations within a geographic theater. Land forces are also defined in JP 3-31, "Personnel, weapon systems, vehicles, and support elements operating on land to accomplish assigned missions and tasks."[6]

Maritime Domain

The maritime domain is defined in Joint Publication (JP) 3-32, *Command and Control for Joint Maritime Operations* as, "The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals."[7] The maritime domain is constrained by land but extends anywhere – on, under or above the water – outside the 12 nautical mile territorial waters boundary. Maritime forces, as defined in JP 3-32, are, "Forces that operate on, under, or above

the sea to gain or exploit command of the sea, sea control, or sea denial and/or to project power from the sea."[8]

Air Domain

The air domain is defined in Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations* as, "The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[9] The air domain, like the land domain, is constrained by the geographic borders of nation states when over land and, like the maritime domain, is constrained by the territorial waters boundary when over water. Air forces, not formally defined in Joint Publications, are manned and un-manned forces that operate in the atmosphere above both land and sea to gain air dominance.

Space Domain

"Space capabilities have proven to be significant force multipliers when integrated into military operations. Space capabilities provide global communications; positioning, navigation, and timing (PNT); services; environmental monitoring; space-based intelligence, surveillance, and reconnaissance (ISR); and warning services to combatant commanders (CCDRs), Services, and agencies."[10]

Definition

The space domain is not formally defined in joint publications, but Joint Publication (JP) 3-59, *Meteorological and Oceanographic Operations*, defines the space environment as corresponding to the space domain, and includes, "…the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere."[11]

There is an entire joint publication, Joint Publication (JP) 3-14, *Space Operations*, dedicated to space operations. JP 3-14 is an excellent document that I reference multiple times in

this paper, however, the most succinct space operations guidance I found is from Air Force Doctrine Annex 3-14, "Space operations involve space superiority and mission assurance."[12] Space superiority, in essence, is controlling the ultimate high ground the space perspective provides.

Boundaries

Space begins at about 50 km above the earth's surface and extends to the edge of the solar system. However, for our purposes, the space domain is constrained between about 160 km where we start to see low earth orbit (LEO) satellites and 35,786 km above the equator where geosynchronous earth orbit (GEO) satellites are parked – although highly elliptical earth orbit (HEO) satellites can reach apogees greater than GEO.

Battlefield

The advantage of operating in space is the space domain provides the ultimate high ground. Space assets orbiting high above the earth's atmosphere provide a large footprint for collecting and disseminating imagery, communications, and signals globally. The space domain has no geographic boundaries. National sovereignty does not extend beyond the earth's atmosphere so satellites are free to cross other nations' borders through space. The space battlefield, therefore, is bounded only by altitude.

The disadvantage of operating in space is the assets are difficult to reach. If a satellite malfunctions and cannot be brought back online through workarounds sent from earth, the payload is generally lost – it is very expensive to retrieve a satellite. Although, technological advances in miniature satellites and alternate launch vehicles are bringing the cost to build, launch and operate satellite systems down.

Laws/Treaties/Restrictions

There are five United Nations treaties governing the use of the space domain.

1. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (The "Outer Space" Treaty).
2. Agreement on the Rescue Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (The "Rescue Agreement").
3. Convention on International Liability for Damage Caused by Space Objects (The "Liability Convention").
4. Convention on Registration of Objects Launched into Outer Space (The "Registration Convention").
5. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (The "Moon Agreement"). [13]

Although there are many detailed articles attached to each, the spirit of treaties two through five is in the titles. The most important treaty – certainly for military consideration – is the Outer Space Treaty. There are nine principles listed under the Outer Space Treaty, but the theme is space should only be used for peaceful purposes.[14]

Forces

Space forces consist of, "The space and terrestrial systems, equipment, facilities, organizations, and personnel necessary to access, use and, if directed, control space for national security."[15]

Cyberspace Domain

"Cyberspace is a domain…not a mission or functional area."

-- Maj Gen Ed Wilson, 24th Air Force Commander

Cyberspace operations allow the United States, and our allies, to gain and maintain a strategic advantage in the operational environment. However, cyberspace access also allows advisories the opportunity to directly and indirectly compromise the integrity of US critical infrastructures ("Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[16]).[17] From Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, "These characteristics and conditions present a paradox within cyberspace: the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular."[18]

Definition

Cyberspace is, "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[19] Cyberspace is an interconnected network of networks located anywhere in the world.

Boundaries

Cyberspace has no boundaries; cyberspace operations cross all domains and borders. The simple cyberspace operations definition from Joint Publication (JP) 3-0, *Joint Operations* is, "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[20] The non-physical uniqueness of cyberspace creates offensive advantages and defensive challenges.

Battlefield

Cyberspace, uniquely, is located in both physical and non-physical domains, within the information environment defined as, "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[21] The cyber battlefield is everywhere.

The advantage and challenge in cyberspace is freedom of action. The Department of Defense, allies, and partner nations have the freedom to pursue and defend against intruders, but adversaries are generally able to attack through cyberspace with little to no consequence for their nefarious activities.

Laws/Treaties/Restrictions

"There are no treaty provisions that directly deal with 'cyber warfare'. Similarly, because State cyber practice and publicly available expressions of *opinio juris* are sparse, it is sometimes difficult to definitively conclude that any cyber-specific customary international law norm exists."[22]

The *Tallinn Manual* was written to identify the international law applicable to cyberwarfare.[23] Although the document is non-binding, it is the best source for understanding how the international law governing the use of force by States and the international law regulating the conduct of armed conflict applies to cyberspace. A weakness of the document is that it does not address cyber criminality.

There is interest in establishing rules for cyberspace operations. Multiple countries, including Russia, proposed a U.N. resolution on a code of conduct to promote peace and security in cyberspace.[24] Also, the United States and China recently agreed to work together and expand cooperation in cybersecurity. Specifically, they agreed to assist with malicious cyber activities; not conduct or support cyber enabled theft of intellectual property; to, "…further identify and

promote appropriate norms of state behavior in cyberspace within the international community…"; and to establish high-level joint dialogue on cybercrime.[25]

Forces

Cyberspace forces execute cyberspace defense, cyberspace operational preparation of the environment, cyberspace intelligence, surveillance and reconnaissance, and cyberspace attack to create the necessary effects in the cyberspace domain.[26]

Command and Control (C2)

Joint Definition

Command and control is defined in JP 1-02 as, "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."[27] This definition is generally sufficient when applied to the air, land and maritime domains, but requires creative application when considered in the unconstrained geographical freedom found in the cyberspace and space domains. For instance, designating "assigned or attached forces" is difficult when considering cyberspace or space assets.

Space

Chapter III in JP 3-14 is devoted entirely to command and control of space forces. The command relationships start with Commander, United States Strategic Command (CDRUSSTRATCOM) who exercises C2 of all assigned and attached space forces through the Commander, Joint Functional Component Command for Space (JFCC Space).[28] "CDRUSSTRATCOM advocates, plans, and executes military space operations and has the responsibility to prioritize, deconflict, integrate, and synchronize military space operations for current and planned joint operations."[29] CDRUSSTRATCOM may delegate operational or

tactical control to the Geographic Component Commanders (GCC) when appropriate, but supporting space forces generally remain assigned or attached to CDRUSSTRATCOM.[30]

Cyberspace

CDRUSSTRATCOM is the authority for both cyberspace and space operations. When conducting cyberspace operations, CDRUSSTRATCOM authorizes Commander, United States Cyber Command (CDRUSCYBERCOM) to manage the routine global operations as the supported commander. When cyberspace operations fall to the theater level the GCC is generally the supported commander. The transition requires coordination, creating a dynamic C2 environment.[31] Further complicating C2 in cyberspace are operations that may require preplanned responses based on triggers that are executed instantaneously if a threat presents.[32]

"When the GCC establishes a subordinate joint command to conduct operations, forces are normally attached as needed, with delegation of OPCON to the subordinate joint force commanders (JFC). However, the GCC also will weigh the operational circumstances and decide if available cyberspace forces/capabilities can be most effectively employed by the subordinate JFC(s), by retaining them at the GCC level, or a combination thereof."[33]

For specific operations, JFCs are designated supported or supporting by the Secretary of Defense and given direction via operations or execution orders.[34] Cyberspace operations within the operational area are conducted through the JFC staff, through the Service component commander or through a functional component commander once the type and availability of assigned cyber forces are considered.[35]

In response to emergent situations, the affected GCC will generally establish a joint task force (JTF) and assign a joint task force commander (JFC). The JFC will first assign theater cyber forces to respond to the threat then request additional forces through SecDef if needed to

augment. The JFC will generally delegate those forces to the service or functional component commanders.[36]

The Problem

Unique characteristics associated with the space and cyberspace domains make command and control within and across these domains challenging. Both domains enjoy access unencumbered by geographic borders. Also, commanders at the tactical and operational level are limited in their ability to command and control either domain.

For example, expeditionary strike groups (ESGs) operate in all five domains. The strike group commander has command and control at the operational level and delegates command and control at the tactical level based on mission. The admiral enjoys nearly unrestricted command and control in the land, maritime, and air domains. The amphibious squadron commander has command and control over the maritime domain before and during the amphibious landing, and then the marine expeditionary unit commander assumes command and control of the land and air domains once Marine Corps units are ashore. The admiral has the freedom to maneuver within these three domains as deemed necessary – the admiral controls the ships, the aircraft and the landing vehicles.

However, the admiral has very limited control over the space or cyberspace domains though operational and tactical success is reliant on both. Line of sight communications are still used at the tactical level, but satellite communications are the standard at the operational level where units are often beyond line of sight with one another. The admiral has no command or control over satellite communication systems. Units request and are granted access to communications satellites at the Geographic CCDR level months in advance of an operation; contingencies are made for emergent tasking, but, absent theater level approval, units are forced

to suffer through mistakes made when requesting satellite access. If an anomaly occurs on a satellite, believed to be caused by an end user, the satellite controller has the authority to deny access to the end user without notice, rebuttal or consideration of the impact to the current operation. The admiral can do nothing but request an explanation, wait for adjudication, and re-submit an access request. Satellite slots are assigned based on perceived priority, the admiral has no control – C2 lies with the combatant commands.

For ships at sea, cyberspace operations are completely reliant on space operations. There are no fiber optic connections from shore to a ship at sea; if the communications path is blocked, cyberspace operations are impossible. The admiral has less command and control in the cyberspace domain than in the space domain, but uses the cyberspace domain (almost exclusively) to command and control in the land, maritime, and air domains. Orders are no longer transmitted by voice, instead (necessarily due to the volume of information required) direction is given digitally. Yet, the admiral is not consulted before "pulling the plug" on space or cyberspace services.

The ESG example is just one of many. Maj Gen Zabel used the ICBM example to highlight C2 challenges and Gen Hyten speaks about the space operations center and the cyberspace operations center cross communications challenges to illustrate the problems with stovepiped data flow.

Where Space Operations Stop and Cyberspace Operations Begin

Before providing clear and concise command and control guidance in the space and cyberspace domains, the boundary between space and cyberspace operations must be identified. I do not believe an absolute physical boundary for cyberspace operations exists – such as roughly

occurs between land, maritime, air and space – but I do believe a conceptual boundary is definable. It is clear that cyberspace touches all domains.

Physical

Pinpointing where space operations stop and cyberspace operations begin is impossible in the physical realm. Though space has physical, definable, boundaries, cyberspace exists in and across all domains. Indeed the joint definition, "A global domain within the information environment…"[37] may be too short sighted as cyberspace extends beyond the globe. Since cyberspace is everywhere, the only possible physical boundary between space and cyberspace is at the limits of the space domain where cyberspace operations within the space domain could be considered space operations and cyberspace operations outside of the space domain could be considered cyberspace operations. Of course this physical boundary definition only works if you don't also consider cyberspace operations within the air, land and maritime domains to be air, land or maritime operations.

Conceptual

Finding a conceptual boundary between space and cyberspace operations is also difficult, but a bit more tenable. If the cyberspace operations definition is expanded to include all data in the information environment (not unrealistic given the Navy Information Warfare Community construct where four information related communities are combined under one umbrella and discussions within the Air Force to tether 24th & 25th Air Force), then space assets exist to enable cyberspace operations. The conceptual boundary between the two domains is where the space mission starts and the cyberspace mission ends.

The Lead (Command) Where Space and Cyberspace Operations Meet

Understanding who has command where space and cyberspace operations meet is important to prevent confusion leading to mistakes. I identified five scenarios where command and control could be designated to either space or cyberspace operations commanders. I believe the solution should be based on the mission focus (cyberspace dominant or space dominant). However, it might be more effective to shift command and control at the overlap point. Another option I considered was assigning command and control based on where the mission originated or terminated.

Space dominant missions have priority

Space dominant missions are those where the mission is space focused; when the space mission is supported and cyberspace is supporting. For example, space dominant missions should have priority when satellites are gathering intelligence, surveillance and reconnaissance information or relaying communications data. During these missions, the space mission commander should have command and control throughout the mission or until a cyberspace dominant mission supersedes.

Cyberspace dominant missions have priority

The reverse should occur when cyberspace dominant missions are supported and space missions are supporting, such as during critical Offensive Cyber Operations (OCO) or Defensive Cyber Operations (DCO). The cyberspace commander should take and maintain command and control throughout the mission or until the mission is superseded by a higher priority space mission. Cyberspace dominant missions would include those that require space assets only for moving data.

Command transfers at the overlap point

When there is no clearly dominant mission or when a mission flips between space and cyberspace supported, command should transfer at the overlap point. This method would enable the most knowledgeable mission commander to take C2 during the mission critical timeframe. The risk with transferring C2 at the overlap point is the potential for dropping the baton at the hand-off, so organizations should strive to maintain C2 throughout missions.

Command based on mission origin point

Another option for command and control when space and cyberspace operations meet is for the geographic commander to assume C2 where the mission originates. This would likely be at the GCC level since neither space nor cyberspace is frequently delegated below the GCC.

For example, if the mission was to conduct cyber operations in North Korea, United States Pacific Command (PACOM), wearing their cyberspace operations hat, would maintain C2 throughout the mission, even if the information crossed into the space operations mission area.

Command based on mission termination point

Similarly, from the mission termination perspective, if United States Northern Command wanted to conduct cyber operations in North Korea, PACOM would maintain C2 throughout the mission since the mission termination point falls in their area of responsibility.

Mission Area Priority When Space and Cyberspace Operations Conflict

The final conundrum I researched was when space and cyberspace missions conflict, but require shared access, which mission commander takes command and control.

Priority mission commander takes command and control throughout the mission

I concluded that the greater mission precedence should have priority and the commander of that mission should assume command and control. When a conflict cannot be resolved by the

mission commanders, the next highest common commander in the chain of command should determine which mission will proceed. At the strategic level, CDRUSSTRATCOM is the authority for both cyberspace and space operations and should adjudicate. At the theater level, the GCC should resolve the dispute.

Recommendations

I offer four suggestions for improving command and control in the space and cyberspace domains. The following proposals are listed in order from least to greatest in cost, effort and time – except for the "Rethink the Problem" section which is meant only to provide a topic for thought.

No Change

There have been no catastrophic events caused by C2 failures in the space or cyberspace domains. Also, change costs time, effort, and money and there is no guarantee a new C2 method would lead to improvement. So, keeping the status quo is a reasonable course of action.

However, this course of action is based on the assumption that the current method is satisfactory, and I believe I have shown that there are at least some areas where change is warranted.

Minor Change

The current system may be adequate, but a few minor adjustments would improve efficiency. First, adjust procedures to improve communication between controllers and users so correct decisions can be made. For example, authorized service interruptions (ASI) are sent out via message traffic. The message contains the units that could be impacted and what the consequences might be. Generally, Echelon IV commands give approval on behalf of their units. The problem is, usually, silence is considered concurrence (*qui tacet consentire videtur*) and

often the potential consequences are profound. Despite the extra effort required, ASIs should require positive approval by impacted units to ensure understanding through communication. This action should be taken by Joint Force Headquarters (JFHQ) Department of Defense Information Networks (DODIN) as the entity established by the Secretary of Defense to, "…achieve unity of command and effort across the full scope of the DODIN."[38]

Second, change policy to ensure space and cyberspace controllers understand the impact their actions will have downstream. Controls should be implemented and enforced to prevent automatic tripwires from creating a greater operational impact than strategic benefit. Commanders should have an opportunity to provide input before decisions are automatically made that will impact their operations.

Third, push control (if not command) to the theater or operational level. Returning to the inbound ICBM scenario proposed by Maj Gen Zabel and detailed in the introduction, communication and understanding are vital to prevent unintended consequences.

Moderate Change

Realign organizations to improve data flow and consolidate knowledge bases – place all cyberspace operations under the same umbrella, separate from space operations. Once complete, remove barriers to free information flow at all levels of space and cyberspace operations. JFHQ-DODIN was established to provide command and control across, "…DOD components that secure, operate and defend the DODIN…"[39] According to the CONOPS, JFHQ-DODIN efforts should optimize C2 across the full scope of cyberspace operations including, "A DODIN C2 framework that is responsive to global and regional priorities."[40]

Integrate across domains at all levels. Endeavor to understand what is important in multi-domain operations, then break the domain stovepipes and integrate. The Commander, United

States Space Command agrees. During a speech at the Air Force Association Air and Space Conference, Gen Hyten said, "General Raymond…You're doing spectacular things and you need to continue to do spectacular things because you're the A3. Because everything we do is a multi-domain problem and you understand all three domains. So for gosh sakes, General Raymond, integrate those domains, push that out across the Air Force, and we're going to make huge progress."[41]

Gen Hyten uses the JSpOC and CAOC to illustrate his point. The two operation centers (OC) pass information back and forth, but they cannot pass data. Shared data to populate a common operational picture in both OCs would pay large dividends to each organization. Gen Hyten also pointed to Cyber and Space Operations Centers, to show he cannot pass data between OCs he owns even though there is a real need to share the data.[42]

Significant Change

Reorganize the military based on domains. The military services were formed with warfare domains in mind. The Army and Navy were formed when conflict was only possible in the land and maritime domains. The Air Force was created following World War II when the impact of warfare in the air domain was significant. Conflict in the space and cyberspace domains is becoming increasingly likely. Establish Space and Cyberspace Forces to prepare for conflict in these domains before adversaries attack. First, redefine each "domain" to eliminate ambiguity – the land domain begins and ends at the water mark where the maritime domain also begins and ends; the air domain is everywhere above the land and maritime domains until the Karman line is reached at the edge of the earth's atmosphere (100 kilometers above sea level); the space domain begins at the Karman line and extends to the edge of the solar system; and the cyberspace domain is everywhere within and across each domain. Then, redistribute domain

specific assets to the newly created Land Force, Maritime Force, Air Force, Space Force, Cyberspace Force, and Support Force. Combine knowledge and resources from each service to maximize forces, and minimize duplicate effort, fighting in each warfare domain.

If establishing Space and Cyberspace Forces is deemed an overreach, create space and cyberspace functional commands to consolidate effort and improve C2 across the DoD in the space and cyberspace domains.

Rethink the problem

Stop classifying space and cyberspace as warfare domains. U.N. treaties prevent nations from weaponizing space. Satellites are not used to cause physical damage to adversaries, they are used only to gather and relay information. Command and control should be at the national level, given the global reach, but should accommodate inputs from the GCCs (who should be consulting with the operational commanders). Command and control does not, however, need to be at the strategic level commanded by a Major Command (MAJCOM).

Cyberspace has no physical boundaries and operates throughout all warfare domains. Cyberspace operations should be conducted as support missions within each warfare domain at the theater, operational and tactical levels. Services should focus efforts on command and control at these levels and leave strategic cyberspace operations to non-military government agencies.

Conclusion

Command and control in space and cyberspace is challenging due to their unique domain characteristics. Both domains have global reach, neither domain is bounded by geographic sovereignty, and operations in the space and cyberspace domains are largely conducted at the strategic level.

Command and control in space and cyberspace is a multi-domain problem, not a space/cyberspace problem. “Where we sit today, we really have very few single-domain problems. All problems are multi-domain problems. So why is it that we struggle so much with realizing that all solutions are multi-domain solutions? They have to be for us to walk that in the future.”[43] “…somehow we make it very, very complicated in space and cyber. And we've got to get to a place where we just look at them as other operational domains that we use and operate and we just move forward. It's not that hard.”[44]

Command and control should be delegated to the lowest level possible and communicated broadly. “The combatant commander is the one “who’s trying to create the battlefield effect,” said Zabel, whether that effect is shooting down an incoming missile or delivering relief supplies. Everything in the Defense Department ultimately should be in service of creating those effects. The COCOM doesn’t command JFHQ-DoDIN, but its mission is to support him, and his will prevails. In any disagreement, Zabel said, “he’s the one who’s going to win.”[45]

Notes

[1] Gen John E. Hyten, "Preserving our Space and Cyberspace Capabilities" (speech, Air Force Association Air and Space Conference, National Harbor, Md., 15 September, 2015), http://www.afspc.af.mil/library/speeches/speech.asp?id=760

[2] Sydney J. Freedburg Jr., "Who Commands In Cyberspace As New HQ Expands?" *Breaking Defense,* 02 September 2015, http://breakingdefense.com/2015/09/who-commands-in-cyberspace-as-jfhq-dodin-expands/

[3] "Who Commands in Cyberspace".

[4] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, 25 March, 2013, X.

[5] Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations*, 24 February 2014, GL-6.

[6] Ibid, GL-6.

[7] Joint Publication (JP) 3-32, *Command and Control for Joint Maritime Operations*, 08 August 2006 Incorporating Change 1, 27 May 2008, GL-11.

[8] JP 3-32, GL-11.

[9] Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*, 10 February 2014, GL-6.

[10] Joint Publication (JP) 3-14, *Space Operations*, 29 May 2013, IX.

[11] Joint Publication (JP) 3-59, *Meteorological and Oceanographic Operations*, 07 December 2012, GL-5.

[12] Air Force Doctrine Annex 3-14, *Space Operations*, 2.

[13] United Nations Office for Outer Space Affairs, *United Nations Treaties and Principles on Outer Space and Related General Assembly Resolutions* (New York: United Nations Publication, 2008), 3-35.

[14] "Space Law Treaties and Principles," *United Nations Office for Outer Space Affairs*, accessed 03 November 2015, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html.

[15] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 12 April 2001 as amended through 17 October 2008, 222.

[16] "DoD Protected Critical Infrastructure Program," *Assistant Secretary of Defense for Homeland Defense and Global Security*, accessed 15 January 2016, http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram.aspx.

[17] Joint Publication (JP) 3-12 (R), *Cyberspace Operations,* 05 February 2013, v.

[18] Ibid.

[19] JP 1-02, 58.

[20] Joint Publication (JP) 3-0, *Joint Operations*, 11 August 2011, GL-8.

[21] JP 1-02, 112.

[22] Michael N. Schmitt, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* 1st ed. (Cambridge: Cambridge University Press, 2013), 5.

[23] *Tallinn Manual.*

[24] Jeremy Kirk, "Russia Pushes for UN Resolution on Cyberspace", IDG News Service, PCWorld, accessed 28 November 2015, http://www.pcworld.com/article/240983/russia_pushes_for_un_resolution_on_cyberspace.html.

[25] "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House Office of the Press Secretary, 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[26] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Issue 73, 2nd Quarter 2014, 14-15.

[27] JP 1-02, 40.

[28] Joint Publication (JP) 3-14, *Space Operations*, 29 May 2013, III-1.

[29] Ibid, III-1.

[30] Ibid, xii.

[31] JP 3-12 (R), x.

[32] Ibid, xi.

[33] Air Force Doctrine Document 3-12, *Cyberspace Operations,* Incorporating Change 1, 30 November 2011, 25.

[34] AFDD 3-12, *Cyberspace Operations*, 20.

[35] Ibid, 25.

[36] Ibid, 25.

[37] JP 1-02, 58.

[38] Joint Force Headquarters (JFHQ) Department of Defense Information Networks (DODIN), *Commander (CDR) JFHQ-DODIN Concepts of Operations (CONOPS) For JFHQ-DODIN,* 15 January 2015, IX.

[39] Ibid.

[40] Ibid.

[41] "Preserving our Space and Cyberspace Capabilities".

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] "Who Commands in Cyberspace".

Bibliography

Air Force Doctrine Document 3-12. *Cyberspace Operations*, 15 July 2010, incorporating change 1, 30 November 2011.

Air Force Doctrine Update. *Domains and Organizing for Joint Operation*, 01 June 2013.

Air Force Future Operating Concept. *A View of the Air Force in 2035,* September 2015.

Air Force Space Command. *High Frontier: The Journal for Space & Missile Professionals Vol. 2, Number 3.* "Space Command and Control." April 2006.

Air Force Space Command. *High Frontier: The Journal for Space & Missile Professionals Vol. 5, Number 3.* "Cyberspace" May 2009.

Alberts, David S., and Richard E. Hayes. *Understanding Command and Control.* DoD Command and Control Research Program, 2006.

Builder, Carl H., Steven C. Bankes and Richard Nordin. *Command Concepts: A Theory Derived from the Practice of Command and Control.* Santa Monica, CA: RAND Corporation, 1999. http://www.rand.org/pubs/monograph_reports/MR775. Also available in print form.

Chamberland, Capt Brian, USMC and Lt Darryl Diptee, USN, "A New Dimension of War: C2 in Cyberspace." *Cutting the Bowwave, Combined Joint Operations from the Sea Centre of Excellence,* 2014: 45-49. https://dl.dropboxusercontent.com/u/18901991/CJOS%20COE%202014%20journal%20-%20A%20New%20Dimension%20of%20War%20-%20C2%20in%20Cyberspace%20(by%20Capt%20Brian%20Chamberlain%20and%20LT%20Darryl%20Diptee).pdf

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12, Cyberspace Operations," 30 November 2011. https://doctrine.af.mil/DTM/dtmcyberspaceops.htm

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-14, Space Operations," 19 June 2012. https://doctrine.af.mil/download.jsp?filename=3-14-Annex-SPACE-OPS.pdf

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-30, Command and Control," 30 November 2011. https://doctrine.af.mil/DTM/dtmcommandcontrol.htm

DoD Protected Critical Infrastructure Program, Assistant Secretary of Defense for Homeland Defense and Global Security, accessed 15 January 2016, http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenseCriticalInfrastructureProgram.aspx.

FACT SHEET: President Xi Jinping's State Visit to the United States, The White House Office of the Press Secretary, 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Freedburg, Sydney J. Jr. "Who Commands In Cyberspace As New HQ Expands?" *Breaking Defense,* 02 September 2015. http://breakingdefense.com/2015/09/who-commands-in-cyberspace-as-jfhq-dodin-expands/

Gertz, Bill, "Russia Flight Tests Anti-Satellite Missile: Moscow Joins China in Space Warfare Buildup," *The Washington Free Beacon,* 02 December 2015, http://freebeacon.com/national-security/russia-conducts-successful-flight-test-of-anti-satellite-missile/

Hyten, Gen John E., "Preserving our Space and Cyberspace Capabilities" (speech, Air Force Association Air and Space Conference, National Harbor, Md., 15 September, 2015), http://www.afspc.af.mil/library/speeches/speech.asp?id=760

Joint Force Headquarters (JFHQ) Department of Defense Information Networks (DODIN), *Commander (CDR) JFHQ-DODIN Concept of Operations (CONOPS) For JFHQ-DODIN*, 15 January 2015.

Kirk, Jeremy, "Russia Pushes for UN Resolution on Cyberspace", *IDG News Service*, PCWorld, accessed 28 November 2015, http://www.pcworld.com/article/240983/russia_pushes_for_un_resolution_on_cyberspace.html.

Limnell, Jarno and Jan Hanska, "The Driving Forces in Cyberspace are Changing the Reality of Security," *Stonesoft*, http://www.stonesoft.com/opencms/export/system/galleries/download/opinion_articles/Stonesoft_DrivingForcesinCyberspace.pdf

National Space Studies Center. "AU-18 Space Primer," September 2009 (second addition). http://www.au.af.mil/au/awc/space/au-18-2009/index.htm

Roader, Tom, "Space Command General Making Changes to Prep for Possibility of Space War," *The Gazette*, 16 November 2015, http://gazette.com/space-command-general-making-changes-to-prep-for-possibility-of-space-war/article/1563440

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* 1st ed. (Cambridge: Cambridge University Press, 2013).

Songip, A. R., Z. Md Zaki, K. Jusoff, J. Prebagaran and Ng. Boon-Beng. "Cyberspace: The Warfare Domain." *World Applied Sciences Journal* 21 (1), 2013: 1-7.

Tyugu, Enn. "Command and Control of Cyber Weapons." *2012 4th International Conference on Cyber Conflict.* NATO CCD COE Publications, Tallinn, 2012: 333-343.

U.S. Joint Chiefs of Staff. *Command and Control of Joint Air Operations.* Joint Publication 3-30. Washington, DC: U.S. Joint Chiefs of Staff, 10 February 2014.

U.S. Joint Chiefs of Staff. *Command and Control of Joint Land Operations.* Joint Publication 3-31. Washington, DC: U.S. Joint Chiefs of Staff, 24 February 2014.

U.S. Joint Chiefs of Staff. *Command and Control for Joint Maritime Operations.* Joint Publication 3-32. Washington, DC: U.S. Joint Chiefs of Staff, 02 August 2006 incorporating change 1, 27 May 2008.

U.S. Joint Chiefs of Staff. *Cyberspace Operations.* Joint Publication 3-12(R). Washington, DC: U.S. Joint Chiefs of Staff, 05 February 2013.

U.S. Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication 1-02. Washington, DC: U.S. Joint Chiefs of Staff, 08 November 2010 as amended through 15 June 2015.

U.S. Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States.* Joint Publication 1. Washington, DC: U.S. Joint Chiefs of Staff, 25 March 2013.

U.S. Joint Chiefs of Staff. *Joint Airspace Control*. Joint Publication 3-52. Washington, DC: U.S. Joint Chiefs of Staff, 13 November 2014.

U.S. Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, DC: U.S. Joint Chiefs of Staff, 11 August 2011.

U.S. Joint Chiefs of Staff. *Space Operations*. Joint Publication 3-14. Washington, DC: U.S. Joint Chiefs of Staff, 07 November 2014.

U.S. Joint Chiefs of Staff. *Unified Action Armed Forces (UNAAF)*. Joint Publication 0-2. Washington, DC: U.S. Joint Chiefs of Staff, 10 July 2001.

United Nations Office for Outer Space Affairs, *United Nations Treaties and Principles on Outer Space and Related General Assembly Resolutions* (New York: United Nations Publication, 2008).

United Nations Office for Outer Space Affairs, *Space Law Treaties and Principles*, accessed 03 November 2015, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html

Welch, Gen Larry D. (ret). "Cyberspace – The Fifth Operational Domain." *Institute for Defense Analysis (IDA)*, 2011. https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf

Wilgenbusch, Ronald C., and Alan Heisig, "Command and Control Vulnerabilities to Communications Jamming," *Joint Force Quarterly*, Issue 69, 2nd Quarter 2013.

Williams, Brett T., "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, Issue 73, 2nd Quarter 2014.